REMARKS

Claims 1-8 are pending in this application. Claim 1 was amended to overcome an objection due to minor informalities. No new matter has been added.

Rejection Under 35 U.S.C. § 102

Claims 1, 2 and 5-8 stand rejected under 35 U.S.C. § 102(e) as anticipated by Drexler U.S. Patent Pub. No. 2003/0079139. Applicant respectfully traverses this rejection.

Applicant's claim 1 recites a cryptographic method during which an integer division of a type q = a div b and/or a modular reduction of a type r = a mod b is performed, where q is a quotient, a is a number containing m bits, b is a number containing n bits, with n less than or equal to m and b_{n-1} is non-zero, b_{n-1} being the most significant bit of the number b, comprising the steps of masking the number a by a random number ρ before performing the integer division and/or the modular reduction, and generating encrypted or decrypted data in accordance with a result of the division and/or modular reduction.

The claimed subject matter concerns a method of integer division or modular reduction secure against covert channel attacks, and in particular differential attacks. The claimed subject matter can be used for performing division operations in a more general cryptographic method, for example a secret or public key cryptographic method. Such a cryptographic method can be implemented in electronic devices such as chip cards, for example.

According to the method, the number a is masked by a random number ρ before performing the integer division and/or the modular reduction. The number a

being masked by a random number, the trace (for example, the energy consumption) left during the execution of the method is different at each execution, so that it is no longer possible to implement a differential covert channel attack. The random number ρ can be modified at each execution of the method, or simply after a predefined number of executions of the method.

According to one embodiment, in order to mask the number a, there is added, to the number a, b times the random number (a <- a + b*ρ). For this purpose, the content of the register b is multiplied by the random number ρ and then added to the number a, and the result of the addition is then stored in the register initially containing the number a. Then the integer division and/or the modular reduction required is next performed.

In the case where an integer division is performed, the result of the integer division performed with the number a masked in the form a+b*ρ is equal to a div b+ ρ. In this case, after the integer division, the contribution made by the random number ρ in order to find the expected result of the integer division on the number a, that is to say a div b, is taken away from the result of the integer division.

In the case where modular reduction is performed, the result of the operation (a+b*ρ) mod b is equal to a mod b, the expected result of the modular reduction on the number a.

Applicant respectfully submits that this same combination of features is neither disclosed nor suggested by Drexler and Falk, viewed alone or in combinations. For example, Drexler discloses encrypting a known message M using a secret key d.

On the other hand, Applicant discloses that a and/or b are secret data, e.g., elements of a key of the method. As discussed, Applicant's method is characterized in that the number a is masked by a random number ρ before performing the integer division and/or the modular reduction. In the cited sections ([0004], [0007] and [0020]) of Drexler, however, it is the known message text M that is "masked" using a random number. There is no teaching or suggestion in Drexler of masking the number a (i.e., Applicant's secret data) by a random number ρ before performing the integer division and/or the modular reduction.

Accordingly, claim 1 is patentable over Drexler, and the rejection should be withdrawn. This logic also disposes of the rejection of claims 2 and 5-8.

Rejections Under 35 U.S.C. § 103

Claims 3 and 4 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Drexler in view of Falk U.S. Patent No. 5,077,793. Applicant also respectfully traverses this rejection. Claims 3 and 4 depend directly or indirectly from claim 1 and are thus also allowable because Drexler is cited for teachings it does not provide. Additionally, Falk, which is cited only for the use of modular subtractors to subtract pseudo-random number sequences from a converted encrypted signal, does not cure the deficiencies of Drexler.

Conclusion

For the foregoing reasons, Applicant respectfully submits that this application is in immediate condition for allowance and all pending claims are patentably distinct

from the cited references. Reconsideration and allowance of all pending claims are respectfully requested.

In the event that there are any questions about this application, the Examiner is requested to telephone Applicant's undersigned representative so that prosecution of the application may be expedited.

If additional fees are required for any reason, please charge Deposit Account No. 02-4800 the necessary amount.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: July 30, 2008

By: /Brian N. Fletcher/
Brian N. Fletcher
Registration No. 51683

P.O. Box 1404
Alexandria, VA 22313-1404
703 836 6620